TrustPort защищает от крипторов-вымогателей

Вред от вымогателей

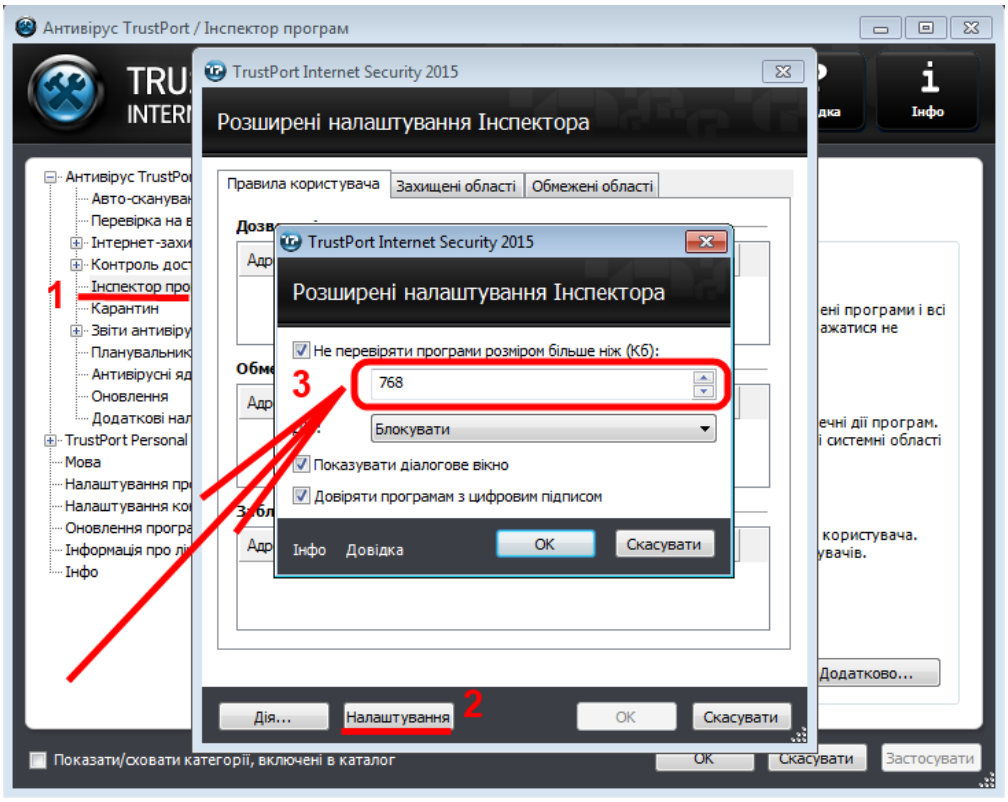
Огромное количество компаний страдает от вирусов-вымогателей (общее название вредоносных программ, предназначенных для вымогания финансов у владельцев зараженных ПК): порнобаннеры, крипторы-вымогатели.

Если вред от порнобаннеров можно считать относительно невысоким (переустановка системы в худшем случае), то крипторы-вымогатели наносят большой ущерб и частным пользователям и коммерческим предприятиям. Крипторы, попадая в ПК, безвозвратно шифруют офисные документы и базы данных, после чего жертве предлагают восстановить зашифрованные документы за довольно солидную сумму: от нескольких сотен до десятков тысяч долларов, зависит от аппетитов хакеров и возможностей пострадавшей компании. Среди пострадавших от крипторов-вымогателей огромное количество предприятий, лишившихся массы документов. Некоторые компании, после ряда безуспешных попыток расшифровать документы, предпочитают заплатить вымогателям (что не является гарантией восстановления информации), ну а остальные компании предпочитают смириться с потерей информации.

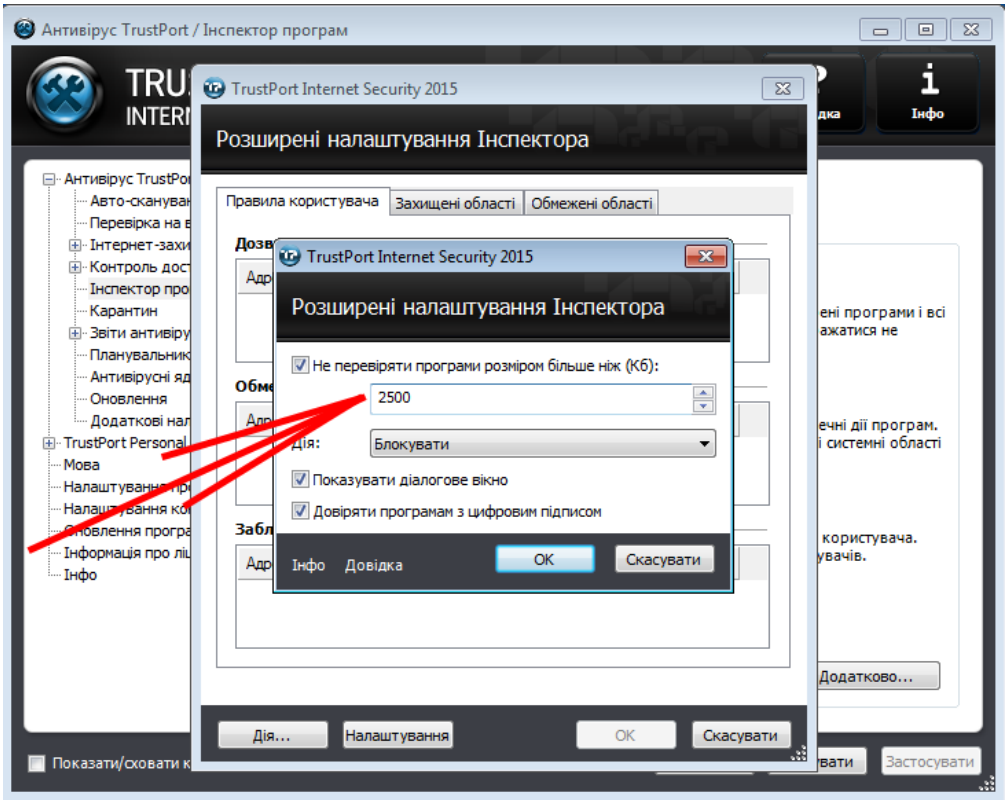
Защита от вымогателей

Избежать заражения вирусами-вымогателями можно используя TrustPort, в функционале которого имеется инспектор приложений, реагирующий на запуск неизвестных программ.

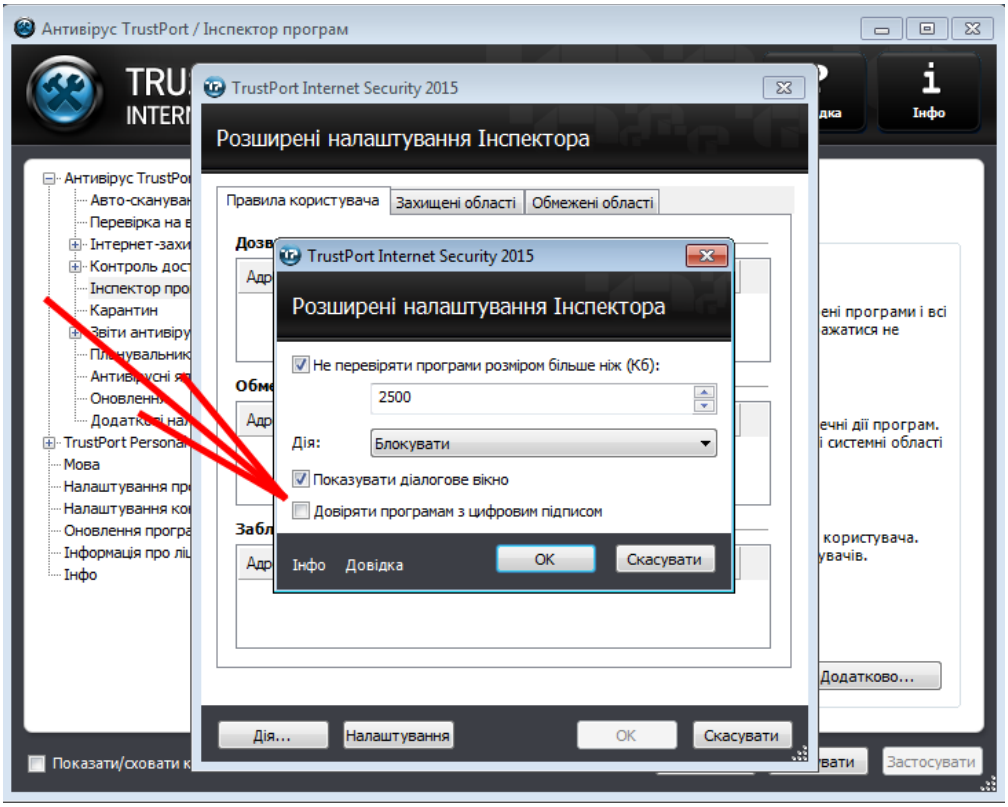
С настройками по умолчанию TrustPort рассчитан на лучшую производительность, поэтому для лучшей защиты наших ПК необходимо немного изменить базовые настройки инспектора приложений. Для этого необходимо открыть окно с настройками антивируса и перейти к настройкам инспектора приложений.



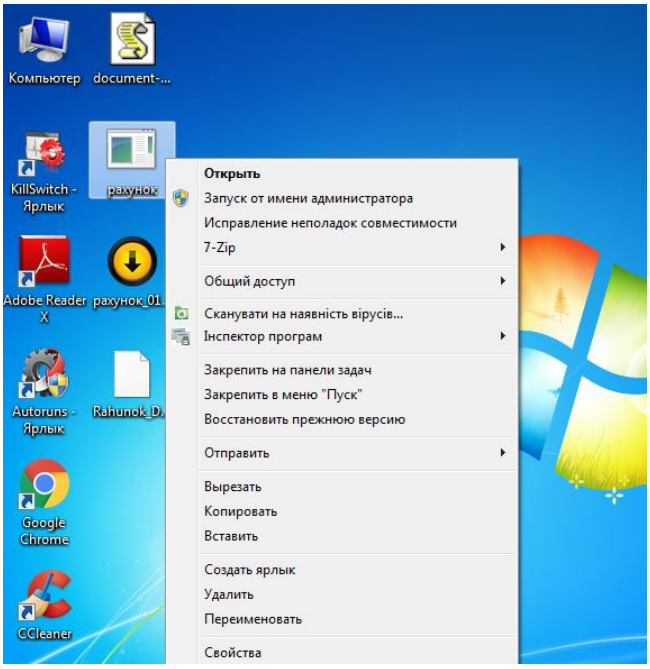
Основная масса крипторов сегодня имеет размер не более 1,5 МБ, поэтому увеличиваем размер программ до 2,5-3 МБ. Применяем настроки.



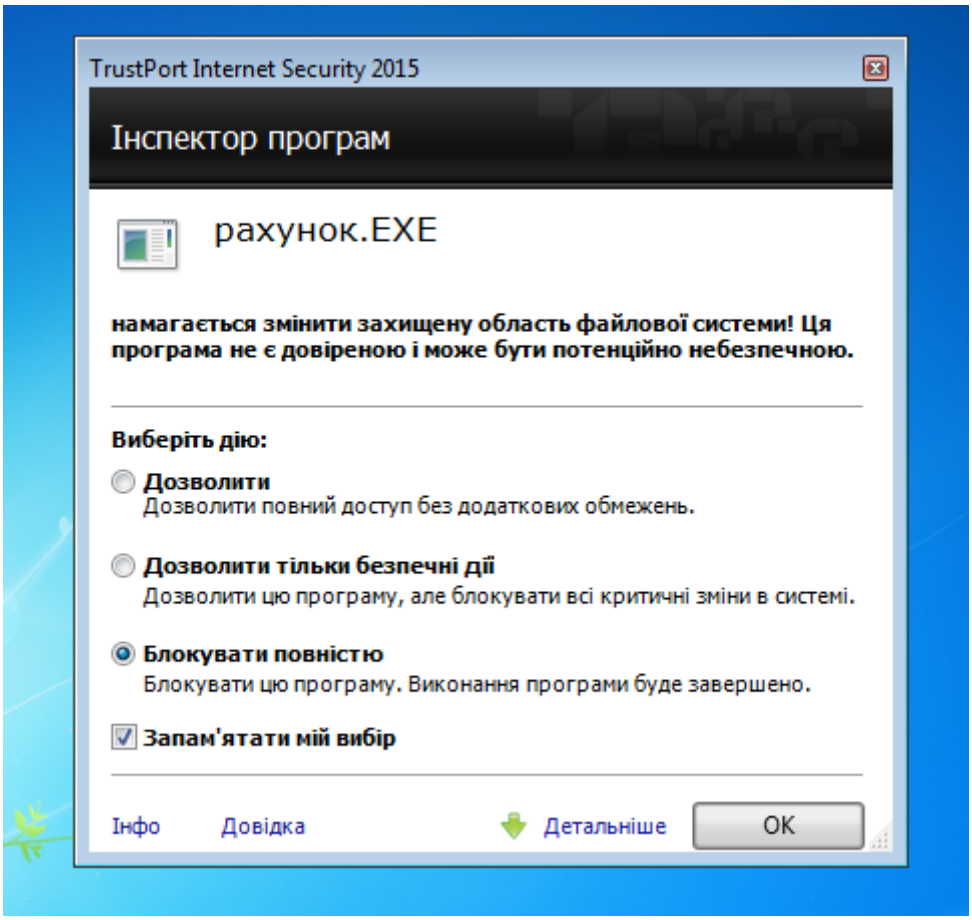
Для продвинутых пользователей можно порекомендовать изменить параметр, в соответствии с которым инспектор приложений определял легальность программы по цифровой подписи, однако в этом случае инспектор приложений переводится на ручное управление и пользователь может получать большое количество запросов.



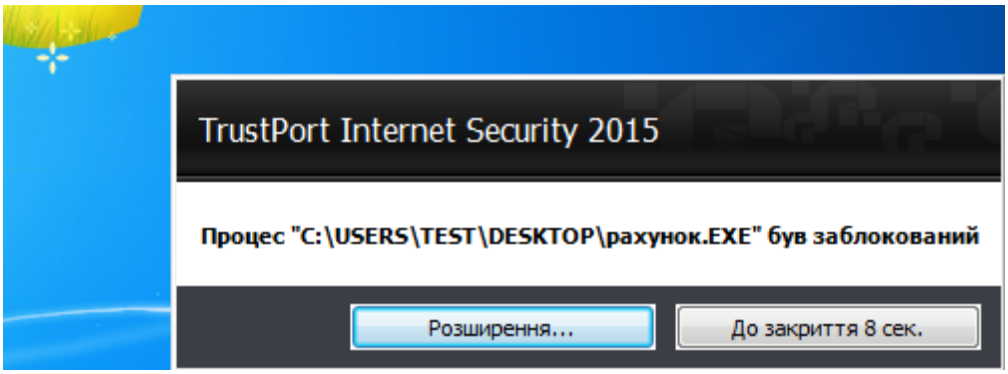
Теперь посмотрим как с этими настройками TrustPort отреагирует на криптор*. Запускаем криптор с правами администратора.



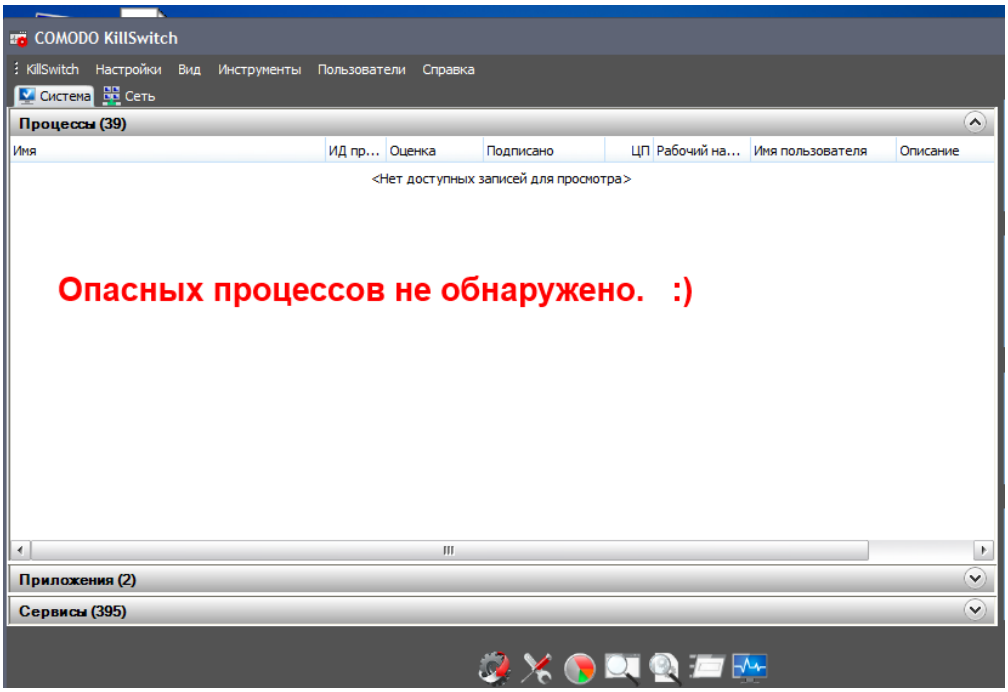
TrustPort остановил выполнение криптора и выдал алерт пользователю, предложив подтвердить выбор «Блокировать полностью». Соглашаемся с инспектором приложений и подтверждаем его выбор.



TrustPort сообщает об успешной блокировке криптора-вымогателя.



Проверяем процессы в системе. Нелегальных процессов не обнаружено.



*Данный тест проводился на тестовой системе. Не рекомендуем повторять тест на реальной системе.